Department of
INFORMATION
TECHNOLOGY

Maryland Continuous Monitoring Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of the executive branch of Maryland State government Information Technology (IT) networks, systems, applications, and data. To provide this level of security within the DoIT Cybersecurity Program, a key component protecting systems and data is the implementation of a continuous monitoring capability.

Within the DoIT Enterprise, the **Security Operations Center (SOC)** is responsible for detecting and identifying anomalies in system and user behavior, ensuring preventive measures are effective and optimized for business and mission functionality, and providing initial response to all cybersecurity incidents. This policy utilizes the standards identified in NIST SP 800-137, SP 800-12, SP 800-53R4, SP 800-61R2, SP 800-92, SP 800-94, and SP 800-152, as well as industry best practices.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 6.7: System and Information Integrity. This policy also supersedes any related policy regarding continuous monitoring declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	**Version**	**Policy Updates**	**Approved By:**
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is focused on the effective implementation of a security operations center within the DoIT Enterprise. The requirements identified under Section 4.0 apply primarily to the Enterprise SOC, but agencies not under the direct management of DoIT (non-Enterprise) may utilize aspects of this policy to institute continuous monitoring capabilities within their agencies.

4.0 Policy

As directed under 2013 Maryland Code § 3A-303 and 3A-305, DoIT is consolidating the IT infrastructure of Maryland Executive Branch agencies. This consolidation aims to standardize hardware and software security and operational requirements to create effective and efficient processes, procedures, and services across the multiple agencies comprising this Enterprise. An inherent part of this SOC implementation is agency-based identification and mitigation of risk. It is DoIT's mission to ensure proper security integration within the IT infrastructure and to fully implement effective detection and prevention security measures without disrupting the wide range of agency missions and business needs.

An operational SOC provides DoIT the ability to detect and prevent network and system exploitation by observing real-time traffic flow behaviors and by correlating log events to baseline trends in near real-time. To effectively manage this information flow and ensure data is protected from both external and internal threats, the State CISO will appoint a Director of

Security Operations. The following subsections describe the policy requirements for event logging, continuous monitoring, incident response, and training and awareness.

4.1 DoIT Security Operations Center

DoIT will establish and implement a SOC staffed with both information security engineers and security analysts to maintain continuous situational awareness of the security posture of the Enterprise. The SOC will be led by a SOC Manager and staffed with analysts equipped to perform the functions listed in the table below.

#	Name	Requirement
A	Director of Security Operations	Government lead of the Security Operation Center with authority to manage resources and will: ▪ Work with the SOC Manager to determine personnel and budget requirements ▪ Lead projects and proof of concepts for security improvements to keep pace with the dynamic threat landscape ▪ Coordinate security with mission and business needs through executives ▪ Develop interagency and external professional relationships to facilitate **cyber threat intelligence (CTI)** sharing and incident response ▪ Oversee forensic protection of evidence relating to incidents in the event of any litigation ▪ Provide overall direction for SOC efforts ▪ Fulfill the role of Maryland Emergency Management Agency (MEMA) Cyber Response Coordinator in the event of a state-wide cyber disruption ▪ Report to the State CISO regarding overall security strategy
B	Monitor Events	The SOC will use automated tools to aggregate traffic data, syslog and event logs, and application and device alerts and logs. These tools will allow security analysts to observe, correlate, and analyze network and system generated data, store required data for historical and analytical purposes, and document anomalies and deviations.
C	Prevent Suspicious Activity	Tune firewalls, intrusion detection/prevention systems (IDS/IPS), and other boundary devices that interact with inbound traffic, both internally and externally, to ensure risks are mitigated in ways that do not adversely affect mission and business functions of the Enterprise agencies.
D	Detect Potential Outbound Malicious Activity	Design and implement methodologies to identify and monitor outbound traffic for indicators of compromise that include detecting increases in endpoint traffic and outbound connections, unauthorized system file changes, increases in data or account access attempts, and other changes in baseline behaviors.
E	Analyze Aggregated Data	Analyze data using baseline comparison, trend analysis, and threat intelligence and implement a forum for documenting alerts and incidents along with maintaining any annotations and corrections made to rulesets or systems.
F	Reporting	Generate and provide tailored reports to the State CISO and other relevant personnel or departments.

4.2 Centralized Analysis Tool

To ensure effective monitoring, Enterprise security analysts must have access to a large amount of network and system data. To parse through that data for threat indicators, an analyst will need to use a centralized logging and analysis capability, such as a System Information and Event Management (SIEM) tool, that allows a comprehensive view of the environment that is efficient and scalable within the network. The table below identifies the functions this tool must be able to perform.

#	Name	Requirement
A	Aggregate Data	The analysis tool must have a robust data schema to aggregate and normalize data across many different devices; this ensures all data can be ingested by the tool for correlation and tracking.
B	Categorize Events	Configure the tool to parse data into an easily understandable format, develop and group events using scripted rules, and seamlessly integrate new devices.
C	Correlate Simple Events	Aggregate events to enable using multiple events to detect otherwise unnoticeable deviations. This allows several events to be correlated and re-evaluated against other alerts.
D	Correlate Multi-Stage Events	Analyze information from a variety of disparate events for any relationship to other events.
E	Prioritize Monitoring And Alerting	Tag targeted assets for special scrutiny, based on the risk or mission-relevance of the asset. Any asset containing or processing confidential information, including financial processing, should generate alerts of the highest priority when monitored.
F	Analyze Statistical Data to Detect Anomalous Behavior	Detect events of significance by identifying mathematical deviations as anomalies from normal traffic such as sharp increases in activity on a particular port, protocol, or event type.
G	Maintain Historical Data and Events	Provide historical or forensic information to determine frame of reference and tracing of any incident over time. This will allow the incident investigator or analyst to go through the data history while tracking the incident and the level of compromise. Data can be reevaluated for compromises that may have gone undetected.
H	Correlate Physical and Logical Events	Make correlations between physical access systems and logical security devices, e.g. operating system logs or VPN data. This allows detection of events and incidents that correlate to alerts like a geographic access violation or suspicious physical activity, such as afterhours building access.

4.3 Continuous Monitoring

During day-to-day operations, the SOC analysts will identify and monitor key threat indicators for:

- Deviations from established operational baselines
- Unauthorized changes to network and system configurations
- Potential security-control violations to network and system devices and applications

The Director of the SOC and SOC Manager will establish comprehensive security requirements the Enterprise that will account for onboarded agency mission and business functions. While a list of criteria required to effectively monitor a network is identified in the table below, it is not an exhaustive list.

#	Name	Requirement
A	Intrusion Prevention	Monitor network boundaries for intrusion attempts, and: ▪ Analyze inbound network traffic to ensure firewall rules are properly tuned to filter unauthorized connections; analyze dropped outbound packets for attempted invalid connections (this may indicate an adversary attempting to establish a command/control channel through an unmonitored port) ▪ Ensure IDSs are configured to balance issues of false positive and false negative alerts and that firewalls and IPSs are not prohibiting legitimate traffic and impeding agency business functions.
B	Outbound Detection	Monitor outbound connections for: ▪ Data exfiltration, ▪ Number and length of unauthorized connections, and ▪ Unauthorized ports and service access.
C	Audit Syslog Events	Review events to detect: ▪ Access control violations, such as an increase restricted file access or internal network connection attempts ▪ The creation and deletion of system and network accounts, which may alert the SOC of an intruder creating an internal account ▪ Assignments of elevated privilege, e.g. group memberships changes, data access permissions
B	Enforce Host Integrity	▪ Enforce file integrity checking on all hosts to ensure system files are not inadvertently changed by users or by unauthorized services ▪ The SOC will monitor the alerts generated by integrity-check-changes which may indicate compromise, e.g. a user clicking on a malicious email
D	Monitor Endpoint Protection	Monitor alerts from endpoint security tools, like antivirus reports and host configuration-change reports.
E	Monitor Cyber Threat Intelligence (CTI) Resources	Maintain active engagement and awareness of current and potential threats by monitoring cybersecurity information feeds, fostering relationships with other cybersecurity entities, and utilizing CTI databases through commercial vendors or government organizations.

4.3.1 Non-Enterprise Agency Guidance

Agencies under the policy authority of, but not directly managed by DoIT, will:

- Review firewall logs daily to
    - Ensure firewalls are tuned properly
    - Look for indicators of external attacks
    - Detect any unauthorized internal-to-external connections

- Monitor for IDS/IPS alerts and respond within an acceptable and identified short period of time so unauthorized intrusions can be identified and reported for remediation

4.4 Incident Response

The DoIT SOC is designated to manage the initial response to any potential cyber security incident. The SOC will review and triage any indications or warnings provided by equipment or personnel. SOC staff will be familiar with the DoIT incident response plan (as well as subscriber agency IR plans (see *Cyber Incident Response Policy*), processes, and procedures and will ensure all incident investigations are managed so as to preserve forensic evidence and ensure a complete record of the incident is available. SOC staff will maintain a well-documented log for any updates and changes to rulesets and listings (e.g. Access Control Lists (ACLs), whitelists, blacklists, firewall rules).

4.5 Training and Awareness

The DoIT SOC will coordinate with the Information System Security Manager (ISSM) to provide cyber security training and awareness for system users (see *Auditing and Compliance Policy*). As part of the yearly training and awareness campaign, system users will be provided information on:

- Current trends in social engineering,
- How to identify potential spam email and texts
- How to identify phishing attacks
- How to report any suspicious activity

The SOC is in a unique position to provide real world examples of these kinds of attacks to non-technical users and help reduce potential threat vectors by ensuring users are aware of their role in protecting the Enterprise systems and data.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Acceptable Use Policy
- Account Management Policy
- Auditing and Compliance Policy
- Cyber Incident Response Policy

7.0 Definitions

Term	Definition
Cyber Threat Intelligence (CTI)	Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
Security Operations Center (SOC)	A division within a cybersecurity program with the purpose of defending against unauthorized activity within computer networks, including monitoring, detection, analysis (such as trend and pattern analysis), incident response, and restoration activities.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for enforcing policies for Enterprise onboarded agencies. DoIT will manage continuous monitoring according to established requirements described in this policy's section 4.0. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies. Any agencies under the policy authority of DoIT with requirements that deviate from the DoIT Cybersecurity Program policies are required to submit a Policy Exemption Form to DoIT for consideration and potential approval.

If DoIT determines that an agency is not compliant with this policy or any supporting policy, the non-compliant agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or authorize a DoIT representative to limit or restrict an agency's access to external and internal communications (effectively shutting down connectivity) until such time the agency becomes compliant.

The Maryland Department of Information Technology is responsible for enforcing policies for all Executive Branch agencies. Any user or agency attempting to circumvent the monitoring capabilities identified in this policy or other supporting policies will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possible criminal and/or civil penalties.